Vefamun'23

United Nations Office on Drugs and Crime

VEFAMUN'23

UNITED NATIONS OFFICE ON DRUGS AND CRIME

STUDY GUIDE: Adressing the issues behind production and distribution of falsified medical products

Table of Contents

Letter From The Secretary General

Most distinguished participants of VefaMUN'23,

After such a prolonged break, as the Secretary-General, I am more than pleased to extend a warm welcome to you at the 4th Vefa Lisesi Model United Nations Conference. After diligent preparation, it is my utmost pleasure to announce that we are ready to host you for one of the premier Model UN conferences. Both our VefaMUN'23 Academic and Organization team has worked tirelessly to cultivate an energetic and engaging atmosphere that will provide the perfect backdrop for tackling some of the world's most pressing issues. I know that your participation in this conference will be just the beginning of a long and meaningful commitment to justice and progress, and we find it to be a privilege to be a part of this journey.

Respectfully,

Ali Kağan Aydıngör, Secretary-General

Letter From The Under Secretary General

Distinguished delegates of VEFAMUN23,

I'm Feyza Çakır and it's a huge honor to be serving as your Under-Secretary-General with Özgur Zaman in our very distinguished UNODC committee and VEFAMUN 2023.

From the first time I started participating MUN conferences, looking for ways to resolve world's problems through negotiating under productive circumstances was my primary drive. MUN provided me an appropriate organization to advance my knowledge about certain aspects of global issues. I experienced compatible diplomatic negotiations and found several opportunities to influence others in significant matters as well as to learn so much from them.

I sincerely believe every delegate here has recognized the importance of the issue drug trafficking and cyber terrorism which affects our world recently and also past years and i also believe that we are the generation that will inherit this deeply corrupted world in the coming years, we have acknowledged and face this issue as soon as we can before it sends the world into flames when we finally have the seat of power.

Finally, I would like to thank my Co-USG, Özgur Zaman for his contributions for the study guide and putting countless effort for you all to have benefit from it. Therefore, we expect you all to use resources including the study guide and others so you can prepare yourself for the committee. We have no doubt that you all going to come up with fruitful solutions for the committee.

Best wishes, Feyza Çakır, Özgür Zaman

INTRODUCTION

A. Introduction to the Committee

The United Nations Office on Drugs and Crime (UNODC) is a global leader in the fight against illicit drugs and international crime. UNODC has approximately 500 staff members worldwide. Its headquarters are in Vienna and it has 21 field offices as well as a liaison office in New York.

UNODC relies on voluntary contributions, mainly from governments, for 90 per cent of its budget. The three pillars of the UNODC work programme are:

• Research and analytical work to increase knowledge and understanding of drugs and crime issues and expand the evidence-base for policy and operational decisions;

• Normative work to assist States in the ratification and implementation of the international treaties, the development of domestic legislation on drugs, crime and terrorism, and the provision of secretariat and substantive services to the treaty-based and governing bodies; and

• Field-based technical cooperation projects to enhance the capacity of Member States to counteract illicit drugs, crime and terrorism. In 1998 the General Assembly gave UNODC the mandate to publish "comprehensive and balanced information about the world drug problem."

Since then, the international community has recognized the importance of detailed, factual and objective information to the field of international drug control. The United Nations Office on Drugs and Crime (UNODC) has published such assessments annually since 1999. This year UNODC introduces its first two volume edition of the World Drug Report, which merges the former Global Illicit Drug Trends publication and the World Drug Report. The consolidation of the two reports is designed to increase the breadth of analytical coverage, while maintaining the annual frequency of statistical output. The first volume covers market trends and provides in depth long term trend analysis, the second volume compiles detailed statistics on all of the drug markets. Together they provide the most complete picture yet of the international drug problem.

The aim of the present Report remains the same as previous years: to contribute to annual assessments by presenting supply (production and trafficking) and demand statistics and analysis on the evolution of the global illicit drug problem. However, by presenting a thorough consideration of the status of the world drug situation and through the presentation of long term trends, this year's report goes further than ever in providing an assessment of the world drug situation.

As in previous years, the present Report is based on data obtained primarily from the annual reports questionnaire (ARQ) sent by Governments to UNODC in 2003, supplemented by other sources when necessary and where available. Two of the main limitations herein are:

(i) that ARQ reporting is not systematic enough, both in terms of number of countries responding and of content, and

(ii) that most countries lack the adequate monitoring systems required to produce reliable, comprehensive and internationally comparable data. National monitoring systems are, however, improving and UNODC has contributed to this process over the last few years. (For more information on data sources and limitations please consult the Methodology section at the end of the report.)

For two decades, the United Nations Office on Drugs and Crime (UNODC) has been helping make the world safer from drugs, organized crime, corruption and terrorism. We are committed to achieving health, security and justice for all by tackling these threats and promoting peace and sustainable well-being as deterrents to them.

Because the scale of these problems is often too great for states to confront alone, UNODC offers practical assistance and encourages transnational approaches to action. We do this in all regions of the world through our global programmes and network of field offices.

B. Introduction to the Agenda Item

UNODC provides evidence on the general situation and trends in the production of opiates, cocaine, amphetamine-type stimulants and cannabis at the global, regional and national levels to strengthen responses to the world drug problem. Its analysis of the drug supply situation is presented in the annual World Drug Report.

To enhance knowledge and support countries in the collection of and reporting on data, UNODC works with Member States to monitor drug cultivation, production and manufacture of cocaine, heroin, cannabis and synthetic drugs / new psychoactive substances (NPS) around the world. UNODC also supports the monitoring of precursors, in collaboration with INCB, and other chemicals used in the illicit manufacture of drugs. The monitoring systems supported by UNODC are tailored to the national contexts and emphasise training and development of local expertise. Collaboration with regional partners, intergovernmental organizations and academic institutions enhances monitoring capacities at national, regional and international levels.

Jointly with the main drug-growing countries in the world - Colombia, Peru and the Plurinational State of Bolivia for coca, Afghanistan, Mexico and Myanmar for opium and Nigeria for cannabis – the UNODC Illicit Crop Monitoring Programme (ICMP) uses GIS and geospatial analysis, satellite imagery and field surveys to monitor the extent and evolution of illicit crop cultivation and production, as well as the factors driving illicit cultivation. The crop and socio-economic surveys help Governments in their policy development and in planning how to tackle illicit drug production. The direct participation of

UNODC in national monitoring systems safeguards transparency of survey and estimation methodologies, ensures international comparability and gives additional credibility to the results.

Besides its activities on drug cultivation and production, UNODC research on drug supply also encompasses activities to monitor and analyse drug trafficking at national, regional and international levels.

C. UN Overview

The World Health Organization (WHO) defines ‘substandard’ medical products as those which are authorised but fail to meet their quality standards or specifications and defines ‘falsified’ medical products as those that deliberately/fraudulently misrepresent their identity, composition or source. Falsification includes substitutions and reproduction and/or manufacturing of an unauthorised medical product. It should be noted that the term ‘counterfeit’ is now associated with intellectual property rights infringements .

Falsified products can apply to both innovator and generic products and may include products without active ingredient, with insufficient active ingredient, with the wrong active ingredient and/or containing other toxic chemicals,

impurities or bacteria. SF medical products have been reported in all main therapeutic categories including medicines, vaccines and in vitro diagnostics. Anti-malarials and antibiotics are the most commonly reported SF medicines . All countries are affected by SF medical products. However, low- and middle-income countries and countries affected by conflict, civil unrest, or with very weak health systems are disproportionately affected.

Globalisation of the pharmaceutical supply chain and access to a global marketplace through a surge in internet connectivity has allowed for many entry points for SF medical products, with some countries identifying a substantial increase in reports in recent years3 . In many countries, the sale of SF medical products is done openly at markets, through unregulated websites, clinics, pharmacies, hospitals and in illegal street markets.

Additionally, The European Commission has been closely involved in several activities that promote this dangerous confusion and pose a threat to access to affordable medicines. EU customs authorities have seized a number of shipments of legitimate generic drugs in transit through the EU to patients in developing countries on the grounds that they might be ‘counterfeit.’ This meant that health staff in developing countries were left scrambling to find medicines so that their patients wouldn’t have their treatment interrupted.

KEY TERMS AND DEFINITIONS

drug trafficking: Drug trafficking is a major source of revenue for organized crime groups, many of whom are involved in other forms of serious crime such as firearms, modern slavery and immigration crime.

generic medicine: A generic medicine is a legitimately-produced medicine that is an exact copy of the originator product and performs in exactly the same way. Generic medicines used in donor-funded treatment programmes and by MSF must meet quality standards to prove they are just as effective as the originator product. Health programmes around the world rely on these affordable copycat medicines.

substandard medicine: A substandard medicine is a drug that does not meet quality standards – it may contain too much or too little of the active ingredient, may be contaminated, may be poorly packaged or fail to meet quality standards in other ways. These medicines may be legitimately-produced mistakes or may have been knowingly produced to a substandard level. Both originator and generic medicines can be found to be substandard, and the issue of substandard medicines is a neglected one that needs far more attention.

fake medicine: A fake medicine is deliberately and fraudulently mislabelled, giving false information on where it was made or by whom, so that people will think it is a legitimate medicine. Fake medicines are dangerous as they are unlikely to contain the active pharmaceutical ingredient needed to make the medicine effective, and may even contain harmful substances. These medicines present a serious threat for public health that needs to be appropriately addressed.

counterfeit medicine: The term ‘counterfeit medicine’ is overly-broad and creates confusion because it conflates intellectual property issues with public health problems. Different organizations and countries use different definitions of the word, making it hard to know exactly which problem is being referred to when this term is used. Some definitions focus on broad intellectual property terms and so confuse legitimate generic medicines with dangerous fakes.

pharmaceutical supply chain: The pharmaceutical supply chain is the means through which prescription medicines are manufactured and delivered to patients. But the supply chain network is actually very complex, requiring a number of steps that must be taken to ensure medications are available and accessible to patients.

chemical substance: A chemical substance is a form of matter having constant chemical composition and characteristic properties.Chemical substances are often called 'pure' to set them apart from mixtures. A common example of a chemical substance is pure water; it has the same properties and the same ratio of hydrogen to oxygen whether it is isolated from a river or made in a laboratory.

DRUG CLASSIFICATIONS AND PUBLIC HEALTH

From common medications to illegal narcotics, drugs abound all over the world. A drug is any substance that alters the physiology, sensation, or cognition of an organism. Since thousands of drugs exist, scientists tend to categorize them into broad classifications on the basis of their shared chemical properties and effects on the human body and mind.

Since many drugs are dangerous and addictive, every country in the world also classifies some drugs or categories of drugs as controlled substances. Drugs become controlled substances when a country's laws restrict people from consuming, possessing, manufacturing, transporting, buying, or selling them within the government's jurisdiction. In some cases, a controlled substance may be illegal for anyone to use for any reason. In other cases, the law may impose limits on how a controlled substance may be used legally, such as exclusively for medical prescriptions or scientific research.

Counterfeit and substandard drugs may contain no active ingredients, less than the required amount of active ingredients, or ingredients not described on the package label. Manufacturers of counterfeit drugs tend to copy more expensive brands of drugs and make them look like brand-name drugs. They may also repackage expired products and substitute a later expiration date, or they may package another drug or alternative substance as if it were an active product. Substandard drugs are made by manufacturers trying to avoid costly quality control and good manufacturing practices; these can result from deliberate or unintended lapses in the manufacturing process. These medicines may have too little or too much of the active ingredients and may not be absorbed properly by the body. If they are taken to treat an illness like malaria, they may be incompletely effective or altogether useless. A counterfeit or

substandard treatment can prolong illness and increase the risk of severe disease or death. If substandard medicines are widely used, they can also select for drug-resistant parasites.

They can be found anywhere, but they are especially prevalent in developing countries lacking effective drug regulatory agencies as well as resources required to effectively evaluate drug quality or enforce drug quality regulations.

Poor-quality medicines present a serious public health problem, particularly in emerging economies and developing countries, and may have a significant impact on the national clinical and economic burden. Attention has largely focused on the increasing availability of deliberately falsified drugs, but substandard medicines are also reaching patients because of poor manufacturing and quality-control practices in the production of genuine drugs (either branded or generic). Substandard medicines are widespread and represent a threat to health because they can inadvertently lead to healthcare failures, such as antibiotic resistance and the spread of disease within a community, as well as death or additional illness in individuals. This article reviews the different aspects of substandard drug formulation that can occur (for example, pharmacological variability between drug batches or between generic and originator drugs, incorrect drug quantity and presence of impurities). The possible means of addressing substandard manufacturing practices are also discussed. A concerted effort is required on the part of governments, drug manufacturers, charities and healthcare providers to ensure that only drugs of acceptable quality reach the patient.

In cases of substandard medication that arise through inadequate production processes, rather than through deliberate falsification of drugs, the lack of quality may be the result of a

variety of factors, including the following: inadvertent use of substandard or incorrect APIs or excipients, poor control of drug quantity, manufacturing processes that cause contamination or do not adequately ensure sterility, and inadequate packaging design or quality. In addition, ineffective quality-control measures, either on the part of the manufacturer or the NMRA, allow such faults to remain undetected.

HIGH INCOME COUNTRIES

Studies in both the UK and Canada show it is a significant issue. Contamination and stability issues were the major problems in Canada, whereas contamination is the major problem in the UK. There were 74 cases of contamination of medicinal products within the UK over an 11-year period and 139 incidents in Canada over a 9-year period. Counterfeit medicines were a minor problem, both in Canada and the UK. An increasing number of substandard medicines have been identified in both Canada and the UK over time, although this may be due to improved detection by regulatory agencies. It is important to note that substandard medicines were not restricted to the manufacturers for generic medicines, but involved all the major pharmaceutical companies in both Canada and the UK.

The clinical impact of substandard medicines is unknown. Contaminated drugs were however responsible for more than 120 deaths at a single hospital in Pakistan. Additionally, more than 700 individuals developed a fungal infection following the use of contaminated methylprednisolone in the USA, associated with at least 61 deaths.

These events suggest that for high-income countries, substandard medicines may be a greater problem clinically than counterfeit medicines. This may also be the situation in lower-income and lower–middle-income countries as illustrated by a study of the Medicines Quality Database (MQDB).MQDB is an online database that documents medicines tested for quality in selected countries in Africa, Asia and South America.A recent study of over 15 000 samples identified 848 samples (5.6%) as being of poor quality.The majority of the failed samples were substandard (767, 90.4%). The remaining 81 (9.6%) were counterfeit.

CONCLUSION

Substandard medicines are medicines which have failed to pass the quality measurements and standards set for them. They should be distinguished from counterfeit (falsified) medicines which are deliberately and fraudulently mislabelled. Combining the together however is not helpful. They are different problems that require different solutions. Substandard and counterfeit medicines are a widespread problem in low-income and lower-middle-income countries. A systematic review showed that the median prevalence of substandard and counterfeit medicines was 28.5%. This ranged from 11% to 48% in individual studies. The 15 studies were all limited to antimicrobial drugs, with the majority (13) including antimalarials. Only 2 of the 15 studies within the systematic review differentiated between substandard and counterfeit medicines. Both studies involved antimalarial drugs in South East Asia. They both found that counterfeit medicines were a greater problem than substandard medicines. The biggest problem in relation to the quality of the medicines tested was an inadequate amount of the active ingredient.

QUESTIONS TO BE ANSWERED

1. What degree of substandard medicines are acceptable?
2. How to raise awareness on the indigent people about medicines?
3. Any possible solution by forming an organisation?
4. How to escape the matrix of major countries' medicine policies?

INTRODUCTION

A. Introduction to the Agenda Item

The United Nations Convention against Transnational Organized Crime defines organized crime groups broadly, encompassing most forms of profit-motivated crime. Aside from its work on specific markets (drugs, trafficked persons, smuggled migrants, firearms, and wildlife), UNODC has conducted a number of regional studies on the full spectrum of organized criminal activities. The political impact of organized crime can include corruption, loss of democratic participation, instability, and conflict. Regional studies have included those in West, Central, and East Africa; East Asia and the Pacific, Central America and the Caribbean, and South-eastern Europe.

Cyber terrorism is defined as a premeditated attack or the threat of such an attack by nonstate actors intending to use cyberspace to cause physical, psychosocial, political, economic, ecological, or other damage. The goal of the cybercriminals is to induce fear or coerce government or nongovernment bodies to act in a way that furthers the criminals' social, financial, or ideological objectives.

A cyber terrorism taxonomy includes six elements:

- An actor or actors with three unique attributes: nonstate, terrorist, and clandestine
- A motive, which may be ideological, social, economic, or political
- An intent to induce or coerce some action, effect change, further objectives, or cause interference

- The means to commit the act, which includes using a computer and network to access cyberspace and cross borders to commit acts of cyber warfare or crimes, including cyberattacks and threats of attacks
- An effect, most commonly violence, service disruptions, physical damages, psychosocial impacts, economic damages, or data breaches
- A target, most commonly civilians, information and communication technology (ICT), data sources, government agencies, nongovernment organizations, or physical infrastructure

B. UN Overview

The UN Office of Counter-Terrorism has several initiatives within the field of new technologies. The Cybersecurity and New Technologies programme aims to enhance capacities of Member States and private organizations in preventing and mitigating the misuse of technological developments by terrorists and violent extremists. This includes countering the threat of cyber-attacks carried out by terrorist actors against critical infrastructure, as well as developing the use of social media to collect open source information and digital evidence to counter online terrorism and violent extremism, while respecting Human Rights.

The programme has also provided expertise in international fora on terrorist uses of unmanned aerial systems

(UAS) and will develop further programming in this area. The project also seeks to mitigate the impact and recover and restore the targeted systems should such attacks occur.

Member States should consider reviewing national legislation to ensure that evidence collected through special investigative techniques or from countries of destination or evidence collected through ICT and social media, including through electronic surveillance, can be admitted as evidence in cases related to foreign terrorist fighters, while respecting international human rights law, including freedom of expression".

Significant points in the development of UNCCT's Cyber Security Programme.

- In 2019, the UN Office of Counter-Terrorism implemented Phase I of the Cybersecurity Programme for South East Asia and Bangladesh, delivering an awareness raising workshop for the 11 beneficiary Member States. A pilot in-depth training workshop was also organized for Thailand, Brunei, Philippines, Bangladesh and Lao PDR.
- In 2020, the UN Office of Counter-Terrorism will implement Cybersecurity Phase I for East Africa, Horn of Africa and the Sahel.

KEY TERMS AND DEFINITIONS

cyber warfare: Cyber warfare occurs when states or international organizations perpetrate hostile acts against other states using cyberspace as a battleground. The acts are committed using malware and other technologies to target the computer systems of governments and businesses. Such attacks constitute an act of war because they are acts of aggression by one state against another.

violent extremism: Terrorism and violent extremism violate the human rights and fundamental freedoms of groups and individuals. However, States define terrorism in different, sometimes ambiguous ways, so domestic legislation does not always protect the human rights of citizens.

THE THREAT OF CYBER TERRORISM

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks

against critical infrastructures could be acts of cyberterrorism, depending on their impact.

Attacks that disrupt nonessential services or that are mainly a costly nuisance would not. It is important to distinguish between cyberterrorism and "hacktivism," a term coined by scholars to describe the marriage of hacking with political activism. ("Hacking" is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Unlike hacktivists, hackers tend not to have political agendas.) Hacktivists have four main weapons at their disposal: virtual blockades; e-mail attacks; hacking and computer break-ins; and computer viruses and worms.

Everyone concerned about the potential danger posed by cyberterrorism is thus well founded. That does not mean, however, that all the fears that have been voiced in the media, in Congress, and in other public forums are rational and reasonable. Some fears are simply unjustified, while others are highly exaggerated. In addition, the distinction between the potential and the actual damage inflicted by cyberterrorists has too often been ignored, and the relatively benign activities of most hackers have been conflated with the specter of pure cyberterrorism.

HISTORICAL BACKGROUND

Small Wars Journal notes that the term "cyber terror" was coined in the 1980s by Barry C. Collin, a research fellow at the

Institute for Security and Intelligence. Collin defined the term as "the convergence of cybernetics and terrorism"; the goal of causing fear and widespread panic has always been at the heart of cyber terror attacks.

The first computer worm transmitted over the internet was the Morris Worm, created in 1988 by Robert Tappan Morris, a student at Cornell University, as the tech site ARN explains. The worm was not intended to be malicious, but an error in its code caused it to become a virus that replicated rapidly and ultimately infected about 6,000 computers. The Morris Worm is estimated to have caused as much as $100 million in damage.

Terrorists soon took advantage of malicious software such as worms to promote their political, social, and economic ends. These are among the earliest events in the history of cyber terrorism:

- In March 1999, the Melissa virus "began spreading like wildfire" across the internet, according to the FBI. Melissa targeted Microsoft's Word word processing software and Outlook email software to automatically send messages to the first 50 people in the victim's contact list. The virus was created by David Lee Smith and was intended not for financial gain but to cause havoc. Melissa damaged email servers at hundreds of corporations worldwide, temporarily knocking out access to about 1 million email accounts.
- In May 2007, government agencies and private businesses in Estonia were the target of massive, weeks-long cyberattacks after the government removed some Russian World War II memorabilia from the city of Tallinn. The distributed denial-of-service (DDOS) attacks caused

Estonia's largest bank to shut down, resulting in about $1 million in damage. Analysts suspect that the Russian Federation supported the attacks, although Russia denies the charge.

- In August 2013, a hacker group called the Syrian Electronic Army took over the websites of the *New York Times*, Huffington Post, and Twitter by breaching the network of MelbourneIT, an Australian internet service provider that manages corporate domain names. The group had previously targeted the websites of the *Washington Post*, CNN, and *Time*. The motivation for the attack was reprisal for criticism of Syrian president Bashar al-Assad.
- In May 2017, the WannaCry ransomware attack struck Microsoft Windows systems, demanding $300 in Bitcoin (later increased to $600) from victims to regain access to their computer files. Months before the attack, Microsoft had issued a patch for the vulnerability exploited by WannaCry, but many users had not updated their system to protect against the attack. A fault in the code of the virus prevented victims from recovering their files even if they paid the ransom.

A significant security trend in recent years is the escalation of the threats posed by cyber terrorism to governments, businesses, and individuals as new technologies are developed. Government Technology reports that the surge in cyberattacks that began in 2020 is continuing in 2021 as attacks become more frequent and more damaging.

THE REASON BEHIND CYBERTERRORISM

The Appeal of Cyberterrorism for Terrorists
Cyberterrorism is an attractive option for modern terrorists for several reasons.

• First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.

• Second, cyberterrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

• Third, the variety and number of targets are enormous. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyberterrorist attack

because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

• Fourth, cyberterrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.

CYBERSECURITY

Cyberattacks can come in the form of viruses, malware, email phishing, social media fraud - the spectrum of cyber threats is limitless. We are more interconnected than ever before, but for all of the advantages, that connectivity leaves us vulnerable to the risks of fraud, theft, abuse, and attack. Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels.

- Organized cybercrime, state-sponsored hackers, and cyber espionage can pose national security risks to our country and our critical infrastructure.
- Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.
- Vulnerability to data breach and loss increases if an organization's network is compromised. Information

about a company, its employees, and its customers can be at risk.

- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

Cybersecurity mandate

During the sixth review of the Global Counter-Terrorism Strategy (A/RES/72/284), Member States expressed concern at the increasing use by terrorists of information and communications technologies (ICT), in particular the internet and other media, and the use of such technologies to commit, incite, recruit for, fund or plan terrorist acts. Member States further noted the importance of cooperation among stakeholders in the implementation of the Strategy, including among Member States, international, regional and sub regional organizations, the private sector and civil society.

In resolution 2341 (2017), the Security Council Calls upon Member States "to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks."

REFERENCES

https://www.unodc.org/unodc/en/data-and-analysis/toc.html

https://online.maryville.edu/blog/cyber-terrorism/#history

https://www.ohchr.org/en/topic/terrorism-and-violent-extremism

https://www.usip.org/sites/default/files/sr119.pdf

https://www.readynh.gov/disasters/cyber.htm

https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity

https://bmjpaedsopen.bmj.com/content/1/1/bmjpo-2017-000007

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4137817/

https://bmjpaedsopen.bmj.com/content/1/1/bmjpo-2017-000007

https://www.cdc.gov/malaria/malaria_worldwide/reduction/counterfeit.html

https://en.wikipedia.org/wiki/Chemical_substancehttps://en.wikipedia.org/wiki/Chemical_substance

https://www.rehabspot.com/drugs/drug-classifications/

https://pharmanewsintel.com/news/fundamentals-of-the-pharmaceutical-supply-chain

https://www.unodc.org/unodc/en/data-and-analysis/drug-cultivation-production-and-manufacture.html

https://www.unodc.org/unodc/en/about-unodc/index.html

https://www.unodc.org/pdf/WDR_2004/Introduction.pdf

https://www.icn.ch/sites/default/files/inline-files/PS_E_Substandard_and_Falsified_Medical_Products_0.pdf

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/drug-trafficking#:~:text=Drug%20trafficking%20is%20a%20major,modern%20slavery%20and%20immigration%20crime.

https://msfaccess.org/spotlight-substandard-counterfeit-medicines